Conexiones inesperadas: comunicaciones inalámbricas, matrices aleatorias y probabilidad libre

Francisco J. Torres Ayala

FC-UNAM,

Seminario de computación científica
16 de febrero del 2017

Conexiones inesperadas

- Eugene P. Wigner, "The Incredible Effectiveness of Mathematics in Sciences", Communications on Pure and Applied Mathematics vol 13, No. 1 (February 1960).

"Conceptos matemáticos aparecen en situaciones totalmente inesperadas "

Comunicaciones Inalámbicas

- Diferentes aspectos:
  - Encriptación.

Comunicaciones Inalámbicas

- Diferentes aspectos:
  - Encriptación.
  - Sincronización.

Comunicaciones Inalámbicas

- Diferentes aspectos:
  - Encriptación.
  - Sincronización.
  - Protocolos de comunicación.

Comunicaciones Inalámbicas

- Diferentes aspectos:
  - Encriptación.
  - Sincronización.
  - Protocolos de comunicación.
  - Transmisión.

Comunicaciones Inalámbicas

- Diferentes aspectos:
  - Encriptación.
  - Sincronización.
  - Protocolos de comunicación.
  - Transmisión.
- Nos vamos a centrar solo en la parte de transmisión.

Comunicaciones Inalámbicas

- Diferentes aspectos:
  - Encriptación.
  - Sincronización.
  - Protocolos de comunicación.
  - Transmisión.
- Nos vamos a centrar solo en la parte de transmisión.
- Queremos una forma de cuantificar cuanta información pasa por el canal de transmisión.

Aleatoriedad

$$\longleftrightarrow \qquad x : \mathbb{N} \to \{\text{Palabras en el libro}\}$$

Aleatoriedad

$$\longleftrightarrow \qquad x : \mathbb{N} \to \{\text{Palabras en el libro}\}$$

- De antemano, no se puede saber el contenido de un libro o qué dira una persona por un celular.

Aleatoriedad

$$\longleftrightarrow \qquad x : \mathbb{N} \to \{\text{Palabras en el libro}\}$$

- De antemano, no se puede saber el contenido de un libro o qué dira una persona por un celular.
- No se conoce x, si no los posible valores de x con un alto grado de probabilidad.

Aleatoriedad

$$\longleftrightarrow \qquad x : \mathbb{N} \to \{\text{Palabras en el libro}\}$$

- De antemano, no se puede saber el contenido de un libro o qué dira una persona por un celular.
- No se conoce x, si no los posible valores de x con un alto grado de probabilidad.
- Se modelan las fuentes de información como variables aleatorias.

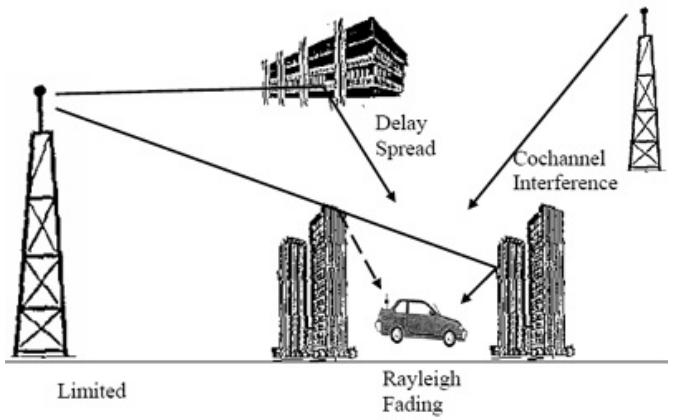
Aleatoriedad

$$\longleftrightarrow \qquad x : \mathbb{N} \to \{\text{Palabras en el libro}\}$$

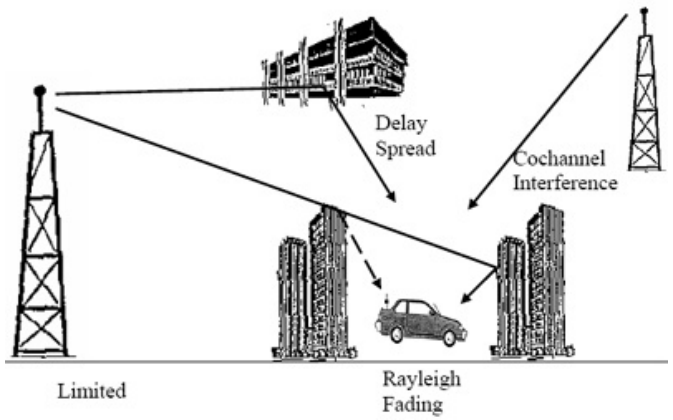
- De antemano, no se puede saber el contenido de un libro o qué dira una persona por un celular.
- No se conoce x, si no los posible valores de x con un alto grado de probabilidad.
- Se modelan las fuentes de información como variables aleatorias.
- Concretamente, una fuente de comunicación es un proceso estocástico

$$(X_n : \Omega \to E)_{n \geq 1}$$

Ruido y Desvanecimiento

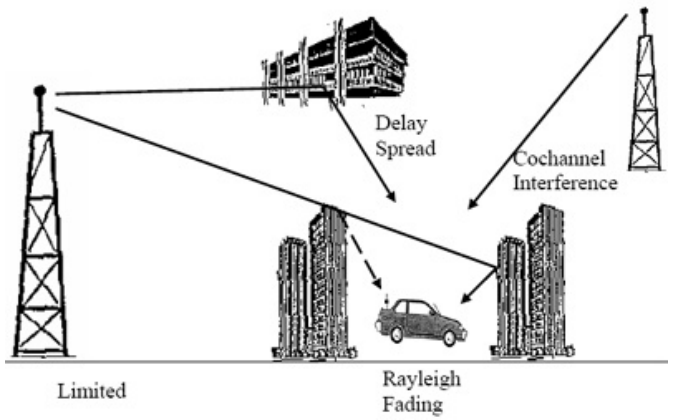


Ruido y Desvanecimiento



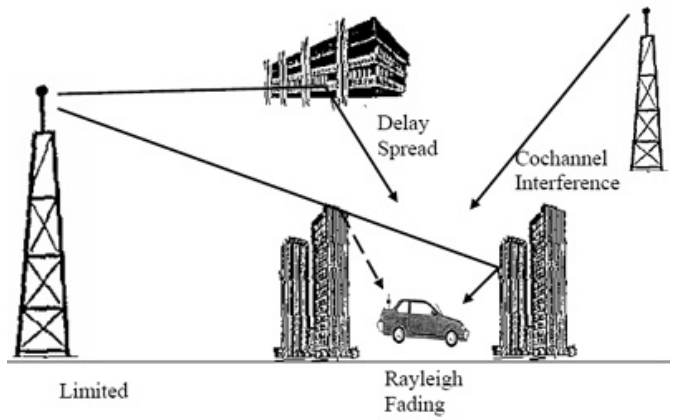
- El mensaje no llegua intacto al receptor.

Ruido y Desvanecimiento



- El mensaje no llegua intacto al receptor.
- Desvanecimiento plano: cambios geográficos y objetos que rodean al transmisor y receptor.

Ruido y Desvanecimiento



- El mensaje no llegua intacto al receptor.
- Desvanecimiento plano: cambios geográficos y objetos que rodean al transmisor y receptor.
- Ruido aditivo: ruido térmico y ruido de disparo (asociado a la radiación electromagnética).

Ruido Aditivo Gaussiano Complejo

Ruido Aditivo Gaussiano Complejo

- El modelo del Ruido Aditivo Gaussiano Complejo

$$Y_n = k_n X_n + \gamma N_n$$

Ruido Aditivo Gaussiano Complejo

- El modelo del Ruido Aditivo Gaussiano Complejo

$$Y_n = k_n X_n + \gamma N_n$$

- Desvanecimiento plano: modelado por k_n, un número complejo.

Ruido Aditivo Gaussiano Complejo

- El modelo del Ruido Aditivo Gaussiano Complejo

$$Y_n = k_n X_n + \gamma N_n$$

- Desvanecimiento plano: modelado por k_n, un número complejo.
- Ruido aditivo: modelado por N_n y $\gamma > 0$. Aqui, N_n es una variable aleatoria normal (media cero y varianza unitaria) y γ es una constante llamada potencia del ruido.

Ruido Aditivo Gaussiano Complejo

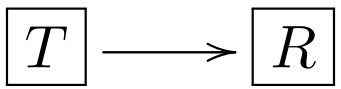
$$\underset{X_n}{\text{señal transmitida}} \longrightarrow \boxed{\text{canal de transmisión}} \longrightarrow \underset{Y_n}{\text{señal recibida}}$$

- El modelo del Ruido Aditivo Gaussiano Complejo

$$Y_n = k_n X_n + \gamma N_n$$

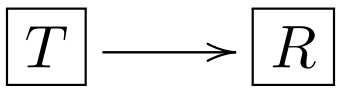
- Desvanecimiento plano: modelado por k_n, un número complejo.
- Ruido aditivo: modelado por N_n y $\gamma > 0$. Aqui, N_n es una variable aleatoria normal (media cero y varianza unitaria) y γ es una constante llamada potencia del ruido.
- X_n y N_n son independientes.

Máxima cantidad de información
Capacidad Ergódica



- ¿Cual es la maxima cantidad de información que puede transmitir el canal de Ruido Gaussiano?

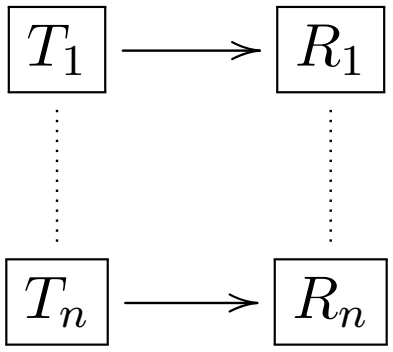
Máxima cantidad de información
Capacidad Ergódica



- ¿Cual es la maxima cantidad de información que puede transmitir el canal de Ruido Gaussiano?
- Con restricciones de potencia, si P es la potencia de transmisión, la capacidad ergódica es:

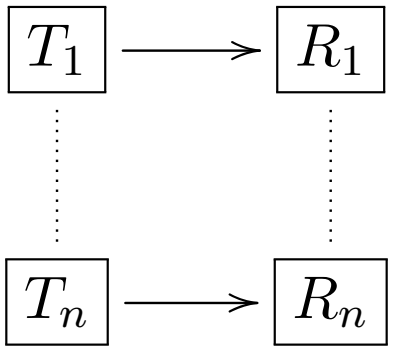
$$C = \ln(1 + P).$$

Divide y ...



- ¿ Que pasa si dividimos la potencia de transmisión en n canales idénticos?

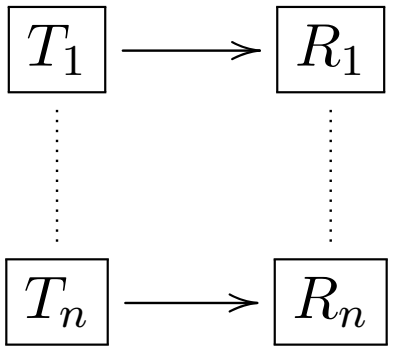
Divide y ...



- ¿ Que pasa si dividimos la potencia de transmisión en n canales idénticos?
- Cada canal aguanta hasta

$$\ln\left(1+\frac{P}{n}\right)$$

Divide y ...



- ¿ Que pasa si dividimos la potencia de transmisión en n canales idénticos?
- Cada canal aguanta hasta

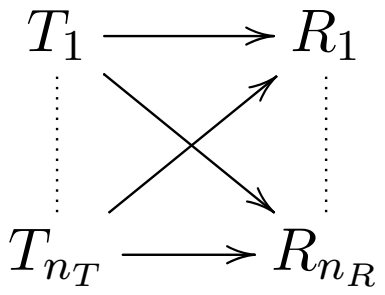
$$\ln\left(1+\frac{P}{n}\right)$$

- En total

$$n\ln\left(1+\frac{P}{n}\right)\to\ln(e^P)=P$$

Sistemas MIMO
(multiple input multiple output)

Sistemas MIMO (multiple input multiple output)



Matrices Aleatorias

$$
\begin{aligned}
Y_n^{(1)} &= \sum_{t=1}^{n_T} k_{1,t} X_n^{(t)} + N_1 \\
&\vdots \\
Y_n^{(n_R)} &= \sum_{t=1}^{n_T} k_{n_R,t} X_n^{(t)} + N_{n_R}
\end{aligned}
$$

- En forma matricial tenemos

$$Y = KX + N$$

- Capacidad del sistema

$$C(n_T, n_R) \approx n_R \, \text{función}(P, \beta)$$

donde $\lim_{n_R \to \infty} \frac{n_T}{n_R} = \beta$ y P es la potencia de tranmisión.

- Capacidad del sistema

$$C(n_T, n_R) \approx n_R \, \text{función}(P, \beta)$$

donde $\lim_{n_R \to \infty} \frac{n_T}{n_R} = \beta$ y P es la potencia de tranmisión.

- Cálculos involucran:

$$\lim_{n_R \to \infty} \frac{1}{n_R} \mathbf{E} \left[\log \det(KXX^*K^* + NN^*) \right]$$

- Capacidad del sistema

$$C(n_T, n_R) \approx n_R \, \text{función}(P, \beta)$$

donde $\lim_{n_R \to \infty} \frac{n_T}{n_R} = \beta$ y P es la potencia de tranmisión.

- Cálculos involucran:

$$\lim_{n_R \to \infty} \frac{1}{n_R} \mathbf{E} \left[\log \det(KXX^*K^* + NN^*) \right]$$

- Observación

$$\log \det(KXX^*K^* + NN^*) = \sum_{k=1}^{n_R} \lambda_k(KXX^*K^* + NN^*)$$

- Capacidad del sistema

$$C(n_T, n_R) \approx n_R \, \text{función}(P, \beta)$$

donde $\lim_{n_R \to \infty} \frac{n_T}{n_R} = \beta$ y P es la potencia de tranmisión.

- Cálculos involucran:

$$\lim_{n_R \to \infty} \frac{1}{n_R} \mathbf{E} \left[\log \det(KXX^*K^* + NN^*) \right]$$

- Observación

$$\log \det(KXX^*K^* + NN^*) = \sum_{k=1}^{n_R} \lambda_k(KXX^*K^* + NN^*)$$

- ¿Cómo se comportan los valores propios de KXX^*K^* y NN^*?

- Capacidad del sistema

$$C(n_T, n_R) \approx n_R \, \text{función}(P, \beta)$$

donde $\lim_{n_R \to \infty} \frac{n_T}{n_R} = \beta$ y P es la potencia de tranmisión.

- Cálculos involucran:

$$\lim_{n_R \to \infty} \frac{1}{n_R} \mathbf{E} \left[\log \det(KXX^*K^* + NN^*) \right]$$

- Observación

$$\log \det(KXX^*K^* + NN^*) = \sum_{k=1}^{n_R} \lambda_k(KXX^*K^* + NN^*)$$

- ¿Cómo se comportan los valores propios de KXX^*K^* y NN^*?
- ¿Se puden obtener los valores propios de $KXX^*K^* + NN^*$ en términos de los valores propios de KXX^*K^* y NN^* ?

Marchenko-Pastur

$$Y_N : \Omega \to M_{N.M}$$

entradas i.i.d. con media cero y varianza finita, σ^2.
Suponiendo $\lim_{N,M\to\infty} \frac{M}{N} = \lambda$.

$$Z_N := Y_N Y_N^*$$

con valores propios $\{\lambda_1, \ldots, \lambda_N\}$.
Distribución empírica da valores propios:

$$\nu_N((a,b)) = \#\{j : \lambda_j \in (a,b)\}$$

Teorema:

$$\lim_{N\to\infty} \nu_N(a,b) = \frac{1}{2\pi\sigma^2} \int_a^b \frac{\sqrt{\lambda_+ - x}\sqrt{x - \lambda_-}}{\lambda x} dx$$

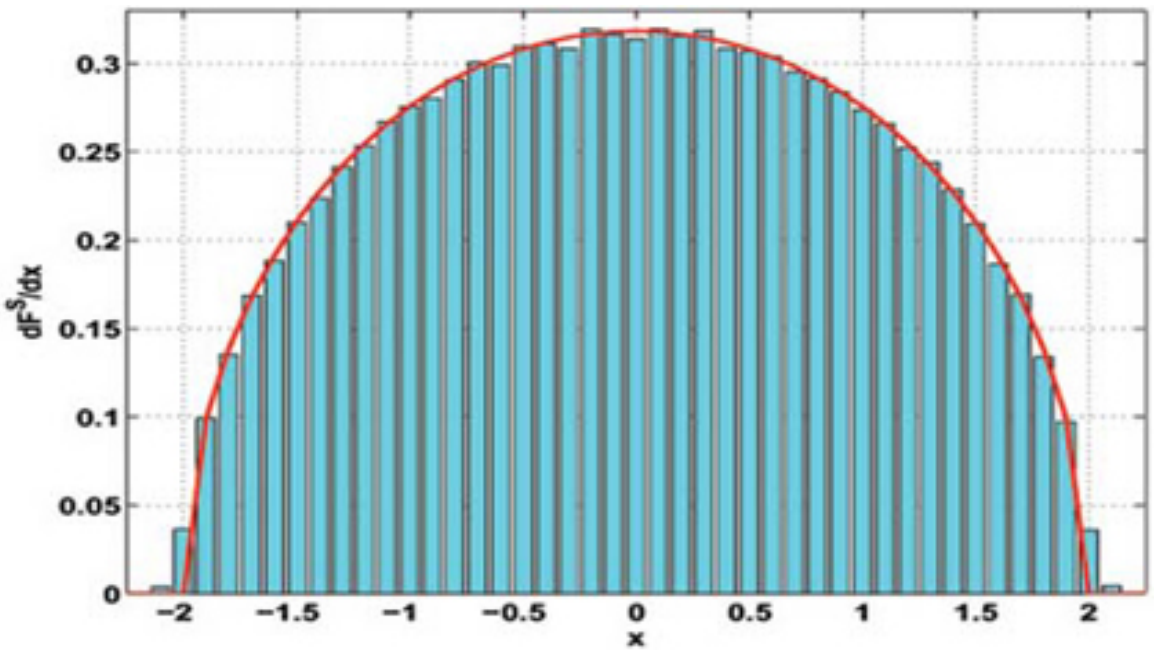
con $\lambda_\pm = \sigma^2(1 \pm \sqrt{\lambda})$.

Teorema del semi-circulo de Wigner

$$Y_N : \Omega \to M_N$$

Y_N, auto-adjunta, con entradas Gaussianas, de media cero y varianza $\frac{1}{\sqrt{N}}$. Entonces, para $p \in \mathbf{N}$

$$\lim_{N\to\infty} \frac{1}{N}\mathbf{P}(a \leq Tr(Y_N^p) \leq b) = \frac{1}{2\pi}\int_a^b t^p\sqrt{4-t^2}dt$$



Abstracción

Encontrar la distribución, asintótica, de valores propios de

$$p(Y_N^{(1)}, \ldots, Y_N^{(r)})$$

donde

- $Y_N^{(i)}$ es una matriz aleatoria de $N \times N$
- p es un polinomio

Espacios de probabilidad no conmutativos

- $\mathbf{B}(H)$, operadores acotados en el espacio de Hilbert H.

Espacios de probabilidad no conmutativos

- $\mathbf{B}(H)$, operadores acotados en el espacio de Hilbert H.

estos juegan el papel de variables aleatorias

Espacios de probabilidad no conmutativos

- $\mathbf{B}(H)$, operadores acotados en el espacio de Hilbert H.

  estos juegan el papel de variables aleatorias

- $\tau : \mathbf{B}(H) \to \mathbf{C}$ un estado, es decir
  1. lineal
  2. $\tau(TT^*) \geq 0$
  3. $\tau(\mathrm{id}_H) = 1$

Espacios de probabilidad no conmutativos

- $\mathbf{B}(H)$, operadores acotados en el espacio de Hilbert H.

  estos juegan el papel de variables aleatorias

- $\tau : \mathbf{B}(H) \to \mathbf{C}$ un estado, es decir
  1. lineal
  2. $\tau(TT^*) \geq 0$
  3. $\tau(\mathrm{id}_H) = 1$

  τ juega el papel de la esperanza $\mathbf{E}$

Espacios de probabilidad no conmutativos

- $\mathbf{B}(H)$, operadores acotados en el espacio de Hilbert H.

  estos juegan el papel de variables aleatorias

- $\tau : \mathbf{B}(H) \to \mathbf{C}$ un estado, es decir
  1. lineal
  2. $\tau(TT^*) \geq 0$
  3. $\tau(\mathrm{id}_H) = 1$

  τ juega el papel de la esperanza $\mathbf{E}$

- $$\tau(p(S_1, \ldots, S_r))$$
  $$\uparrow$$
  $$\frac{1}{N}\mathbf{E}[Tr(p(Y_N^{(1)}, \ldots, Y_N^{(r)}))]$$

Libertad

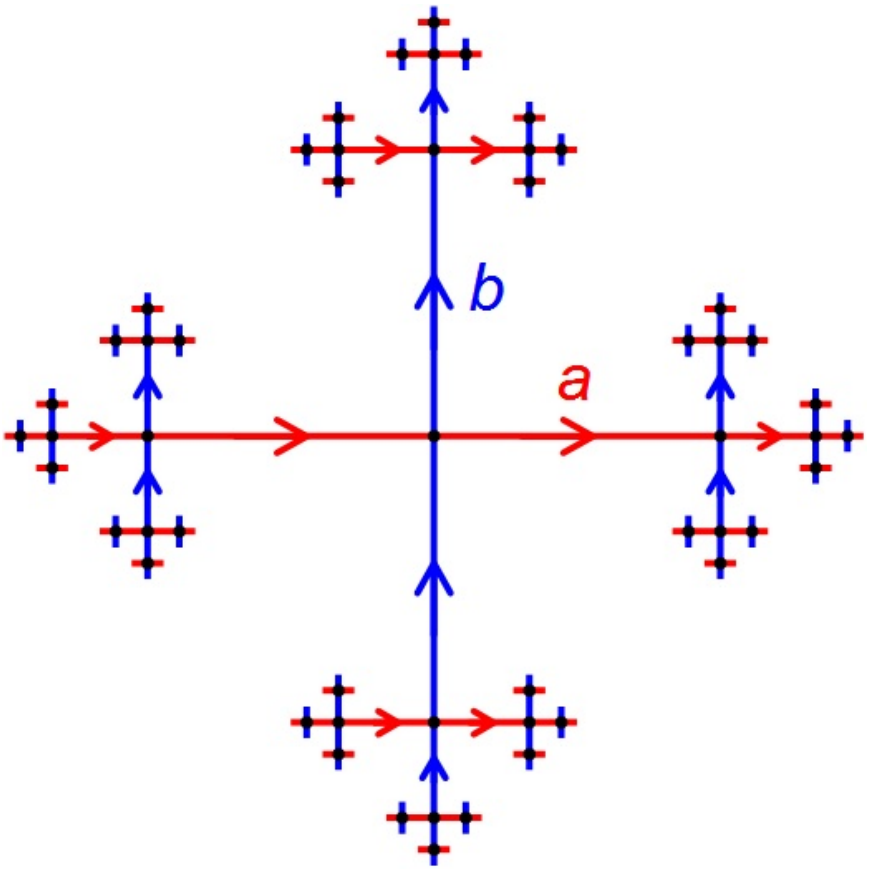
- ¿Cómo se reemplaza la independencia ?
- Tomar una familia de sub álgebras con uno, $\{A_i\}_{i\in I}$, de $\mathbf{B}(H)$, cerradas bajo adjunción.
- $\{A_i\}_{i\in I}$ se llama libre si siempre que se tienen elementos $a_{i_1} \in A_{i_1}, \ldots, a_{i_n} \in A_{i_n}$ con
  - (alternante) $i_1 \neq i_2, \ldots, i_{n-1} \neq i_n$
  - (centrada) $\tau(a_{i_j}) = 0$, para toda j

  Entonces

$$\tau(a_{i_1} \cdots a_{i_n}) = 0$$

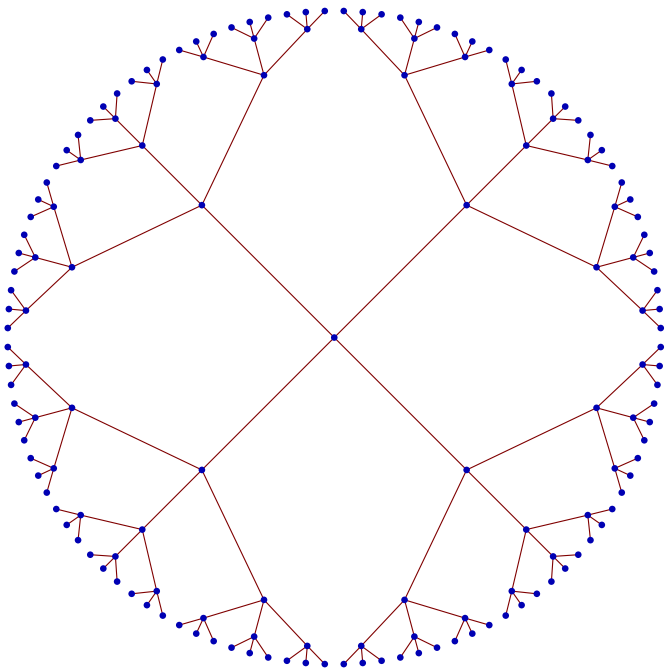
El origen de la probabilidad libre

- Estructura de álgebras de operadores.
- En especial álgebras de von Neumann asociadas a grupos libres.

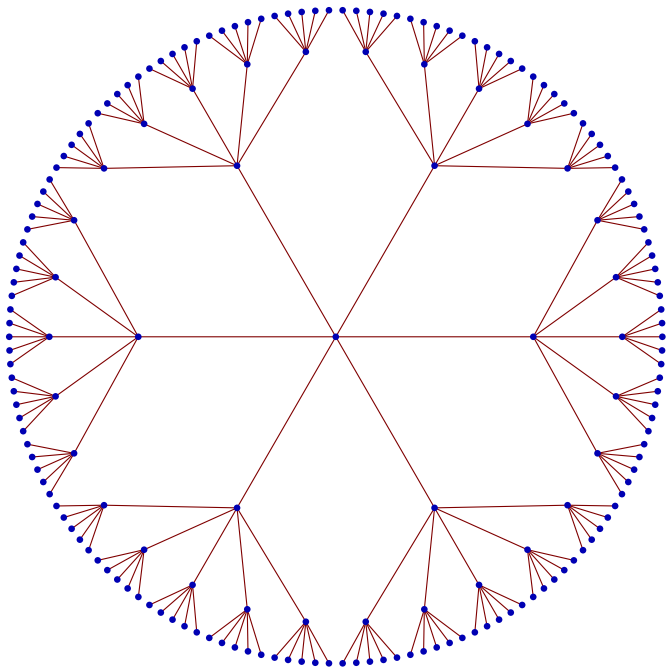


Gráficas de Cayley de grupos libres

Grupo libre
de rango 2

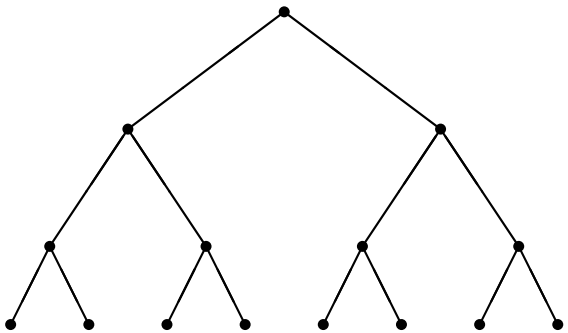


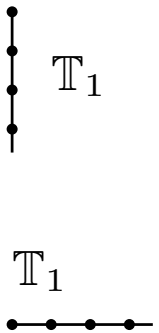
Grupo libre
de rango 3

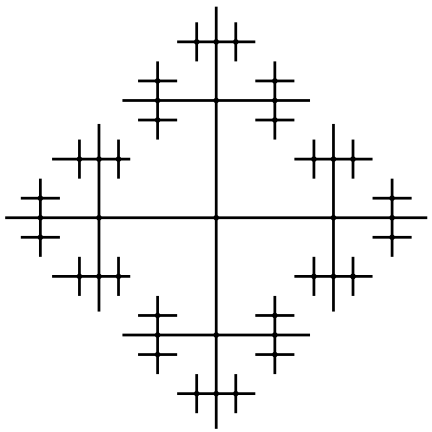


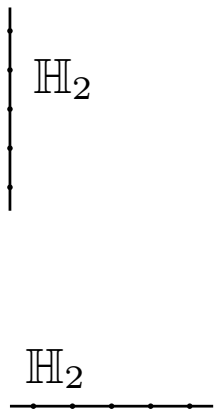
Otro ejemplo

- Aspectos combinatorios (de cierto tipo) de gráficas infinitas.









Gracias